International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 05 Issue: 08 | Aug - 2021 ISSN: 2582-3930

Review paper on Secure Sharing of Personal Health Records in Cloud

Jive Komal Dilip[1], Dr.S.B.More[2], Prof.A.H.Syed[3], Dr.P.S.Kadu[4]

[1]Department of Post Graduation (Software Engineering), Aditya College of Engineering, Beed, MS, India
[2]Department of Post Graduation (Software Engineering), Aditya College of Engineering, Beed, MS, India
[3]Department of Post Graduation (Software Engineering), Aditya College of Engineering, Beed, MS, India
[4]Department of Post Graduation (Software Engineering), Aditya College of Engineering, Beed, MS, India

---

Abstract - In emerging world of cloud computing gives wide range of functionalities. Personal Health Record (PHR) enables patients to store, share, and access personal health data in centralized way that it can be accessible from anywhere and anytime .Storing the confidential health information to cloud servers is not secure, there is issues such as revelation or theft of data and there is need for the development of methodologies that ensure the privacy of the PHRs. Therefore, we use methodology called SeSPHR for secure sharing of the PHRs in the cloud. The SeSPHR scheme ensures patient centric control on the PHRs and preserves the confidentiality of the PHRs. The patients store the encrypted PHRs on the un-trusted cloud servers and selectively grant access to different types of users on different portions of the PHRs. A semi-trusted proxy called Setup and Re-encryption Server (SRS) is introduced to set up the public/private key pairs and to produce the re-encryption keys. The methodology is secure against insider threats and also enforces a forward and backward access control.

Key Words: Cloud computing, personal health record, Re-encryption Server, Secure Sharing of Personal Health Records, Encryption.

1. INTRODUCTION

Cloud computing has emerged as an important computing paradigm to offer pervasive and on-demand availability of various resources in the form of hardware, software, infrastructure, and storage Consequently, the cloud computing paradigm facilitates organizations by relieving them from the protracted job of infrastructure development and has encouraged them to trust on the third-party Information Technology (IT) services. Additionally, the cloud computing model has demonstrated significant potential to increase coordination among several healthcare stakeholders and also to ensure continuous availability of health information, and scalability.
Generally, the PHRs contain information, such as: (a) demographic information, (b) patients' medical history including the diagnosis, allergies, past surgeries, and treatments, (c) laboratory reports, (d) data about health insurance claims and (e) private notes of the patients about certain important observed health conditions. More formally, the PHRs are managed through the Internet based tools to permit patients to create and manage their health information as lifelong records that can be made available to those who need the access.

With the help of SeSPHR methodology communication and interaction between patients and PHR users. PHR users are pathologist, radiologist, doctors, pharmacist, friends and family. Storing the private health information to cloud servers managed by third parties is not secure .there is possibility of access of unauthorized person. There is major risk to store and maintain privacy of the PHRs stored in public clouds that are managed by commercial service providers. The PHRs are stored on the third-party cloud storage; they should be encrypted in such a way that neither the cloud server providers nor the unauthorized entities should be able to access the PHRs

A methodology called Secure Sharing of PHRs in the Cloud (SeSPHR) is used to administer the PHR access control mechanism managed by patients themselves. The methodology preserves the confidentiality of the PHRs by restricting the unauthorized users. Generally, there are two types of PHR users in the proposed approach, namely: (a) the patients or PHR owners and (b) the users of the PHRs other than the owners, such as doctors and physicians, health insurance companies' representatives, pharmacists, radiologist, pathologist and members or friends of patients. The patients as the owners of the PHRs are permitted to upload the encrypted PHRs on the cloud by selectively granting the access to users over different portions of the PHRs.

In contrast to the approach presented in that pro-poses the management of multiple keys by the PHR owners, which eventually leads to overheads at the PHR owner's end, the SeSPHR methodology avoids the over-head by delegating the SRS for setting up the public/private key pairs and producing the decryption keys for the authorized users only. The methodology considers the cloud servers as the un trusted entity and therefore, introduces a semi-trusted server called the Setup and Re-encryption Server (SRS) as the proxy. Proxy Re-encryption based approach is used for the SRS to generate the re-encryption keys for secure sharing of PHRs among the users. The PHRs are encrypted by the patients or PHR owners and only the authorized users having the keys issued by the SRS can decrypt the PHRs. Moreover, the users are granted access to the specific portions of PHRs as deemed important by the PHR owner. This methodology is more secure because the users are granted access to the specific portions of PHRs.

2. PROPOSED SYSTEM

The proposed scheme employs proxy re-encryption for providing confidentiality and secure sharing of PHRs through the public cloud. The proposed methodology to share the PHRs in the cloud environment involves three entities namely:
(a)The cloud
(b) Setup and Re-encryption Server (SRS) and
(c) The users.

The Cloud: The scheme proposes the storage of the PHRs on the cloud by the PHR owners for subsequent sharing with other users in a secure manner. The cloud is assumed as un-trusted entity and the users upload or download PHRs to or from the cloud servers. As in the proposed methodology the cloud resources are utilized only to upload and download the PHRs by both types of users, therefore, no changes pertaining to the cloud are essential.

Setup and Re-encryption Server (SRS): The SRS is a semi-trusted server that is responsible for setting up public/private key pairs for the users in the system. The SRS also generates the re-encryption keys for the purpose of secure PHR sharing among different user groups. The SRSin the proposed methodology is considered as semi-trusted entity. Therefore, we assume it to be honest following the protocol generally but curious in nature. The keys are maintained by the SRS but the PHR data is never transmitted to the SRS. Encryption and decryption operations are performed at the users' ends. Besides the key management, the SRS also implements the access control on the shared data.

Users: Generally, the system has two types of users:
(a) The patients (owners of the PHR who want to securely share the PHRs with others) and
(b)The family members or friends of patients, doctors and physicians, health insurance companies' representatives, pharmacists, and researchers. In SeSPHR methodology, the friends or family members are considered as private domain users whereas all the other users are regarded as the public domain users. The users of both the private and public domain may be granted various levels of access to the PHRs by the PHR owners.
The PHR is logically partitioned into the following four portions: Personal Information, Medical information, Insurance related information and Prescription information.

Methodology Proposed System

The proposed SeSPHR methodology comprises of the steps namely: Setup, Key generation, Encryption and Decryption.

Setup: The proposed methodology works on groups G1 and $G2$ with the prime order q. The bilinear mapping of $G1$ and $G2$ is $G1 \times G1 \rightarrow G2$. A parameter g is a random generator such that $g \in G1$.The variable Z is another random generator such that $Z = (g, g) \in G2$.

Key Generation: The public/private key pairs are generated by the SRS for the set of authorized users. The keys are generated as following:

$$SKi = x, i = gxi$$

Where $xi \in Zq*$. The SKi and PKi represent the private and public key of user i, respectively. The keys are securely transmitted to the corresponding users.

Encryption: Suppose any patient P needs to upload his/her PHR onto the cloud. The patient client application generates random number(s) equal to the PHR partitions placed in the distinct access level groups by the user. In our case, we consider that all of the four partitions described in Section 2 are at different access levels. Therefore, in our case four random variables $r1$, r2, $r3$, $r4 \in Zq*$ are generated. The variable ri is used to encrypt ith partition of the PHR. Each partition is encrypted separately by the client application. The XML format conveniently allows the application to perform encryption/decryption on logical partitions of the PHR. The encryption of the aforesaid partitions of the PHR is performed as follows.

$$Cper = Zr1.PHRper$$

Where PHRper refers only to the personal partition of the PHR and Cper is the semi-encrypted file that contains the personal partition as encrypted text.

$$Cins = Zr2.PHRins$$

Where $PHRins$ refers only to the insurance partition of the PHR and $Cins$ is the semi-encrypted file that contains the insurance partition as encrypted text in addition to the $Cper$ that was encrypted in the previous step.

$$Cmed = Zr3.PHRmed$$

Where $PHRmed$ refers only to the medical information partition of the PHR and $Cmed$ is the semi-encrypted file that contains the insurance partition as encrypted text in addition to the Cper and Cins that were encrypted in the previous steps.

$$C = Zr4.PHRpres$$

Where$PHRpres$ refers only to the prescription information partition of the PHR. Here, C represents the complete encrypted file that contains all the partitions in the encrypted form. Therefore, we have not used the sub-script with the last step of encryption. It is noteworthy that the sequence of encryption may be changed and the above given sequence is not hard and fast.

In addition to the above stated encryptions, the client also calculates the following parameters.

$$Rper\_P = gr1xp$$
$$Rins\_P = gr2xp$$
$$Rmed\_P = gr3xp$$
$$Rpres\_P = gr4xp$$

Where xp is the private key of the patient that is uploading the PHR. The parameter R is used to produce the re-encryption key for the partition indicated in the subscript of each R.The P in the subscript shows that the parameter R is generated by the user P. The completion of the encryption phase is followed by the upload of complete encrypted file C to the public cloud. The parameters $Rper\_P$, $Rins\_P$, $Rmed\_P$, and $Rpres\_P$ are transmitted to the SRS along with the file identification for which these parameters are generated.
It is noteworthy that a patient after registering with the SRS needs to send at least the following information to get the aforementioned parameters.
• Number of partitions of PHR
• Label of each partition, for instance personal information, medical information, insurance information, and prescription information
• Role that has access to any particular partition (any role may be given access to more than one partitions), like doctors may be given access to medical in-formation
•Initial members of family/friends to give access

Decryption: Suppose a user U desires to access the encrypted PHR (C) uploaded by the patient P. The user U downloads the C directly from the cloud (after the cloud authentication process). Afterwards the user Urequests the SRS to compute and send the corresponding R parameters that are used for decryption. The SRS checks the ACL for the requesting user

and determines whether the access to the partition for which the user has requested *R*, is granted by the PHR owner or not.

According to the access permissions specified in the ACL, the SRS will generate the corresponding parameters and will send those to the requesting user.

3. WORKING MODULES

We have provided following Modules into our working system:

Module 1: Data Owner (Patient)

- Patient module involves tiny wireless sensors that are embedded inside or surface-mounted on the body of a patient.
- These sensors continuously monitor the vital physiology parameters of the patient such as body temperature, pulse rate and also monitor the saline level. Collected personal health data are aggregated and transmitted via wireless interface to the cloud.

Module 2: Data User

- Doctors, nursing staff, pharmacies, clinical laboratory personnel, insurance providers, and the service providers is the data users in Health network.
- In SeSPHR, a data uses resource-limited terminals to generate secret keys and conduct the information retrieval operation.
- The secret keys are sent to the public cloud via wireless channel and the retrieved PHR files are returned. Then, the data user decrypts the PHR files and verifies the correctness of decryption.

Module 3: Public cloud

- The public cloud has almost unlimited storage and computing power to undertake the PHR remote storage task and respond on data retrieval requests.
- Lightweight test algorithm is designed in our proposed system to improve performance.

Module 4: Key Generation Center (KGC)

- KGC generates public parameters for the entire system and distributes secret keys to data users. A data users set of attributes is embedded in his secret key to realize access control.
- If a traitor sells his secret key for financial gain, the KGC is able to trace the identity of the malicious user and revoke his secret key.

4. CONCLUSION

- We proposed a procedure to safely store and transmission of the PHRs to the authorized elements in the cloud.
- The strategy preserves the security of the PHRs and authorizes a patient-driven access control to various segments of the PHRs on the access provided by the patients.
- The PHR owners store the encrypted information on the cloud and just the approved users having valid re-encryption keys issued by a semi-trusted authority can decrypt the PHRs.
- The job of the semi-trusted authority is to produce and store the public/private key sets for the clients in the system.

REFERENCES

1. M. H. Au, T. H. Yuen, J. K. Liu, W. Susilo, X. Huang, Y. Xiang, and Z. L. Jiang, “A general framework for secure sharing of personal health records in cloud system,” Journal of Computer and System Sciences, vol. 90, pp, 46-62, 2017
2. A.Abbas, K. Bilal, L. Zhang, and S. U. Khan, “A cloud based health insurance plan recommendation system: A user centered approach, “Future Generation Computer Systems, vols. 4344, pp. 99-109, 2015.
3. M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, “Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption,” IEEE Transactions on Parallel and Distributed Systems, 2013, vol. 24, no. 1, pp. 131–143.
4. J. Li, “Electronic personal health records and the question of privacy,” Computers, 2013, DOI: 10.1109/MC.2013.225.
5. T. S. Chen, C. H. Liu, T. L. Chen, C. S. Chen, J. G. Bau, and T.C. Lin, “Secure Dynamic access control scheme of PHR in cloud computing,” Journal of Medical Systems, vol. 36, no. 6, pp. 4005– 4020, 2012.
6. Z. Xiao and Y. Xiao, “Security and privacy in cloud computing,” IEEE Communications Surveys and Tutorials, vol. 15, no. 2, pp. 1– 17, Jul. 2012.
7. . Wu, G.-J. Ahn, and H. Hu, “Secure sharing of electronic health records in clouds,” In 8th IEEE International Conference on Collaborative Computing: Networking, Applications and Work sharing (CollaborateCom), 2012, pp. 711-718
8. A. N. Khan, ML M. Kiah, S. A. Madani, M. Ali, and S. Shamshirband, “Incremental proxy re-encryption scheme for mobile cloud computing environment,” The Journal of Supercomputing, Vol. 68, No. 2, 2014, pp. 624-651.
9. D. C. Kaelber, A. K. Jha, D. Johnston, B. Middleton, and D. W. Bates, “A research agenda for personal health records (PHRs),” Journal of the American Medical Informatics Association, vol. 15, no. 6, 2008, pp. 729-736.